

Humboldt State University Confidentiality Statement for Employees, Consultants, and Independent Contractors Accessing University Records

Personally identifiable information and other confidential data include, but are not limited to, an individual's Social Security Number (SSN), date of birth (DOB), home address, home telephone number, academic performance record, financial data, physical description, medical history, disciplinary history, gender, ethnicity, and religious preference.

While Humboldt State University employees, consultants, and independent contractors may have exposure to records that contain personally identifiable information and/or other confidential data, they are PROHIBITED from viewing any such data in any University record without written approval in advance by the campus President or Vice President for Administrative Affairs.

SECTION TO BE COMPLETED BY EMPLOYEE, CONSULTANT, OR INDEPENDENT CONTRACTOR

I certify that I have read and understand the attached "Summaries of Provisions of the California Information Practices Act of 1977 and California Penal Code Section 502."

I certify that, in order to ensure the privacy and security of data, I agree to:

- Access, distribute, share, and retain confidential data only as authorized and only as needed to conduct campus business as required to perform my job duties.
- Store under secure conditions all confidential data that I retain and ensure its confidential and timely destruction when no longer needed to conduct campus business as required by my job.
- Respect the confidentiality and privacy of individuals whose data I access.
- Observe any ethical restrictions that apply to data to which I have access.
- Protect confidential information located at my workstation.
- Report immediately to my supervisor any and all apparent and suspected security breaches.
- Comply with all department and campus security policies and procedures.

I certify that I agree NOT to:

- Discuss verbally or distribute in electronic or printed formats any confidential data except as authorized and as needed to conduct campus business as required to perform my job duties.
- Make unauthorized copies of confidential data.
- Knowingly falsely identify myself.
- Gain or attempt to gain unauthorized access to confidential data or University computing systems.
- Share my user ID(s) and password(s) with anyone nor use anyone else's user ID(s) or password(s), except as authorized.
- Leave my workstation unattended and unsecured while logged-in to University computing systems.
- Use or allow other persons to use University data for personal gain.
- Engage in any activity that could compromise the security or confidentiality of data held in University records.

I certify that I have read this Confidentiality Statement and that I understand it.

_____ Employee's Name (print)	_____ Signature	_____ Date
_____ Title	_____ Department	

SECTION TO BE COMPLETED BY MANAGER

My signature below certifies that the above employee, consultant, or independent contractor, who is under my supervision, may require access to personally identifiable information and/or other confidential data about students, faculty, staff, alumni, applicants, patrons, contributors, or other individuals in the performance of his or her job duties.

_____ Manager's Name (print)	_____ Signature	_____ Date
---------------------------------	--------------------	---------------

SECTION TO BE COMPLETED BY PRESIDENT OR VICE PRESIDENT FOR ADMINISTRATIVE AFFAIRS

I approve the above Humboldt State University employee, consultant, or independent contractor being granted access to confidential data in Humboldt State University's records to the extent needed to conduct campus business as required to perform his or her job duties. I reserve the right to revoke this approval at any time should I have reason to believe its continuance could compromise data confidentiality, security, or integrity.

The actual creation of computer log-in accounts for this employee, consultant, or independent contractor to access confidential data requires specific authorization by the appropriate "data owner" as that term is defined in Humboldt State University's Appropriate Use Policy. The data owner may require additional certifications of agreement and understanding prior to granting such authorization.

_____ Dr. Rollin Richmond, President	_____ Date
---	---------------

OR

_____ Carl Coffey, Vice President for Administrative Affairs	_____ Date
---	---------------

**Summaries of Provisions
of the
California Information Practices Act of 1977 and California Penal Code Section 502**

INFORMATION PRACTICES ACT OF 1977

Article 10. Penalties

1798.55 – The intentional violation of any provision of this chapter or any rules or regulations adopted thereunder, by an officer or employee of any agency shall constitute a cause for discipline, including termination of employment.

1798.56 – Any person who willfully requests or obtains any record containing personal or confidential information from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than five thousand dollars (\$5,000), or imprisoned not more than one year, or both.

CALIFORNIA PENAL CODE SECTION 502

Section 502 is intended to provide protection to individuals, businesses, and governmental agencies such as Humboldt State University from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems.

502 Computer crimes – Status as felonies:

- (b) Any person who intentionally accesses or causes to be accessed any computer system or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or extort or (2) obtaining money, property, or services with false or fraudulent intent, representations, or promises shall be guilty of a public offense.
- (c) Any person who maliciously accesses, alters, damages, or destroys any computer system, computer network, computer program, or data shall be guilty of a public offense.
- (d) Any person who violates the provisions of subdivision (b) or (c) is guilty of a felony and is punishable by a fine not exceeding five thousand dollars (\$5,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both such fine and imprisonment, or by a fine not exceeding two thousand five hundred dollars (\$2,500), or by imprisonment in the county jail not exceeding one year, or by both such fine and imprisonment.

– End of Summaries –

ADDITIONAL INFORMATION SOURCES

Further information on applicable state and federal laws can be obtained at the following Web site locations:

- Information Practices Act of 1977
<http://www.privacy.ca.gov/code/ipa.htm>
- California Code of Regulations – Title V
<http://ccr.oal.ca.gov>
- Family Educational Rights and Privacy Act (FERPA)
<http://www.ed.gov/offices/OM/fpco/ferpa/>
- CSU Coded Memorandum HR2002-27 – Requirements for Protecting Confidential Data
<http://www.calstate.edu/HRAdm/pdf2002/HR2002-27.pdf>
- CSU Coded Memorandum HR2003-5 – Requirements for Protecting Confidential Data - Updated
<http://www.calstate.edu/HRAdm/pdf2003/HR2003-5.pdf>
- CSU Records Access Manual (February 2003)
http://www.calstate.edu/Gc/Docs/Records_Access_Manual.doc

HUMBOLDT STATE UNIVERSITY APPROPRIATE USE POLICY

The Humboldt State University Appropriate Use Policy is available on the Humboldt State University Web site at

<http://www.humboldt.edu/~its/planning/policy/aup.html>